年末年始における
サイバーセキュリティ注意点

01. 12月中に対応いただきたいこと

＜基本対策！各種アップデートの実施＞

アップデートを行い「**最新状態を保つこと**」がセキュリティ対策における基本です。
休暇に入る前に確実に済ませておきましょう！

PC端末（Windows/Mac）
スマートフォン タブレット
サーバ（ADサーバ/ファイルサーバ等）
ウイルス対策ソフト
VPN機器
Webブラウザ（Chrome、Edge等）
各種ソフトウェア
・Web会議ツール(Zoom等)
・リモート操作ツール（TeamViewer等）
・画像編集ソフト‥等

＊ ＊ ＊ **それぞれのアップデートが最新状態になっているかを確認しましょう！** ＊ ＊ ＊

＜各種アカウント管理の見直し＞

- ✓ **不要なアカウントが残っている場合は削除する**
- ✓ **会社名・名前等の安易なパスワードの設定を利用している場合は見直し**
- ✓ **二段階認証(※)などの設定の有効化もおすすめ**

(※)SMSメッセージで受信した番号を入力する等、IDパスワード入力後に追加で確認を行う仕組み

未使用アカウントは残っていませんか？
（例：クラウドサービスのアカウント、VPNユーザーアカウント、Webサイト管理アカウントなど）
放置された未使用アカウントや弱いパスワードを狙うサイバー攻撃が増加しています。
休暇前に確認を行い、パスワードの変更や不要アカウントの削除を検討しましょう。

02. 休暇に入る前日に対応いただきたいこと

＜使わないものは確実なシャットダウンを＞

万一既に攻撃者に侵入されている場合でも、
インターネットに繋がらなければ何もできません。

- ✓ **パソコンの電源は全てOFFにする**

→Wi-Fi機能もオフにしておきましょう。スリープモードはNGです。

- ✓ **年末年始に社内アクセスしない（VPN機器にアクセスしない）場合はVPN機能を無効にする**
- ✓ **社内にあるサーバ(ADサーバ、ファイルサーバ等）も、可能な限り電源をOFFに**
- ✓ **確実にバックアップ取得されていることを確認し、可能なものはオフライン環境へ（ネットワークから外し、オフライン環境にする）**

→オフライン、もしくはクラウドバックアップがお勧めです。

03. 休暇中の注意点

＜PCは利用はせず、ゆっくり休みましょう＞

休日中は、日常的なサポートを受けられない前提で、
休みの日はPCを立ち上げずに休みましょう。

- ✓ **自宅Wi-Fiルータのファームウェアのアップデートを最新状態にする**
- ✓ **メールの添付ファイルやURLは安易にクリックしない**

04. 会社初めの日に対応いただきたいこと

- ✓ **各種アップデート対応**

→OS、ソフトウェア、ウイルス対策ソフト、Webブラウザ等、
休暇中にアップデートプログラム等が出ているかもしれません。
確認し、再度最新状態へ更新を行いましょう。

- ✓ **ウイルス対策ソフトにてマルウェアスキャン**

→既知のウィルスを駆除できる可能性があります。
実施したうえで年始のお仕事をはじめましょう！

- ✓ **大量に届いているメールの処理に気をつける**

→仕事初めの日は、大量に届いているメールを確認することから始めると思います。
特に添付ファイルは安易に開封せずに電話等で確認をし、
問題ないと認識してから開きましょう。

- ✓ **オフラインバックアップを元に戻す**

→ネットワークのケーブルを外している場合はケーブルを
接続しましょう。

05. 緊急連絡先の確認

＜万一の際の連絡体制は整備されていますか？＞

不測の事態が発生した場合に備えて、委託先企業を含めた
緊急連絡体制や対応手順等を確認しておきましょう。

以上を参考に、安心して年末年始休暇をお過ごしください。

CISO
Chief Information Security Officer